The European Data Protection Board and a number of data protection authorities in EU Member States have issued guidance on how to safeguard EU-US data transfers post-Schrems II.

The General Data Protection Regulation (GDPR) and its predecessor laws have always relied on a basic key principle as far as international data transfers are concerned: adequacy. Any transfers of personal data outside the European Union to a third country whose data protection regime is not considered adequate to protect the rights of data subjects, such as the United States, must therefore be restricted.

The aim has always been to ensure that the rights of EU data subjects are not compromised when their data is sent outside the region. The GDPR contains a number of mechanisms for compensating shortcomings in the recipient country laws. For US transfers, the most common mechanisms have been standard contractual clauses (SCC) approved by the European Commission, or self-certification to the EU-US Privacy Shield.
On 16 July 2020, in a case commonly referred to as Schrems II, the Court of Justice of the European Union (CJEU) issued a landmark ruling that invalidated the Privacy Shield on the basis that the US legal regime governing access to personal data by national security agencies does not contain adequate limitations and safeguards. The CJEU also held that SCCs were sufficient to protect personal data, but that a case-by-case assessment was required of the data protection standards provided in the destination jurisdiction.

GUIDANCE FROM EU AUTHORITIES

Current guidance from EU authorities, including the European Data Protection Board (EDPB), does not provide a fully secure solution to complying with Schrems II. Instead it merely offers a protocol based on a new key principle of GDPR: accountability. To that end, the EDPB lists a combination of measures that can be implemented by data exporters to have effective control over the data they transferred overseas.

Businesses may enter into one of the current sets of SCCs templates issued in 2001 and 2004 and then amended in 2010, and may then strengthen the SCCs with additional contractual commitments to safeguard personal data, such as including a more aggressive obligation on data importers to notify their data exporters when they are required to provide data access to local authorities. To be effective, however, local laws must allow the data importer to provide such notification to the data exporter.

The EDPB also suggests that certain organisational measures can be used to effectively safeguard personal data post-transfer. These measures may consist of internal policies and procedures that provide the steps a data importer can take to challenge disproportionate or unlawful requests by local authorities and to provide transparent information to data subjects. These procedures should be supported by
training sessions that take into account the specific notice and reporting requirements under the data importers’ local laws.

There are some interesting congruencies between the EDPB’s recommendations for how to secure personal data transfers and the US the Health Insurance Portability and Accountability Act (HIPAA), which regulates the use and disclosure of protected health information in order to protect patient privacy. For example, de-identification plays a major role under both legal systems as a technique to mitigate the privacy risk to data subjects. Of course, pseudonymisation does not release the parties from their obligations under the GDPR, but it will effectively reduce the privacy risk in many circumstances, especially if the data exporter retains sole control of the algorithm or repository that enables re-identification.

In addition to the EDPB guidelines, a number of Member States have issued their own guidelines or opinions specific to health data transfers. The German authorities have adopted a strict approach to data transfers that prohibits digital health applications from processing personal (patient) data in the United States. The German authorities also explicitly prohibit the use of tools or other services provided by companies that still rely on their Privacy Shield certification to process personal data in the United States.

France adopted a similar approach to the German authorities, in response to the large media coverage about the use of Microsoft as a hosting provider for France’s centralised public health database, the Health Data Hub. The French Minister for Health subsequently enacted an order banning the transfer of COVID 19-related personal data outside France.

When conducting their assessment as required under the Schrems II ruling, data exporters in the European Union can also rely on solutions from courts such as the French Administrative Supreme Court. In its 19 June 2020 decision analysing the risks associated with potential requests from US courts/authorities under the Clarifying Lawful Overseas Use of Data (CLOUD) Act to access data hosted within the European Union by an affiliate of a US entity, the Conseil d’Etat opined that the CLOUD Act provisions did not create a major or urgent risk for health data protection.

Businesses should carry out a data mapping exercise that identifies all cross border transfers.

Regarding the risk associated with Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12 333, the Conseil d’Etat ruled on 13 October 2020 that, given the important public interest of maintaining a COVID 19 health database, the risks of access by US authorities, although possible, are not serious enough to justify the suspension of the service and the immediate change of provider.

**STEPS TO COMPLY WITH DATA TRANSFER GUIDANCE**

The most immediate action that businesses can take is to understand the extent to which health data is transferred from the European Economic Area (EEA) to the United States and other counties not deemed to have an adequate data protection
regime. To do this, businesses should carry out a data mapping exercise that identifies all cross border transfers and the mechanism used to validate them.

Once these transfers have been identified, businesses should then undertake a data transfer assessment that identifies the inherent risks and whether any supplemental measures should be applied to protect the health data post-transfer. It is important to note that branches or subsidiaries of US cloud service providers are not the only entities that may be covered by US surveillance laws. To some extent, an EU parent company that stores health data in the European Union might be subject to US authorities’ access requests if one of its affiliates is established within the European Union and has some form of control over the data. A thorough analysis of the applicability of foreign surveillance laws to any provider should thus be conducted during a data transfer assessment.

Because health data is sensitive in nature, businesses should take extra care when assessing what technical and organisational measures are prudent to protect against surveillance. Businesses may consider additional technical safeguards, such as pseudonymisation and encryption in transit and at rest, as well as organisational safeguards like explicit contract provisions that permit onsite/remote audits and, if applicable, prohibitions on the sharing of data with companies that are subject to FISA 702.

Particular care should also be taken where health data can be transferred onward to a third party and where a sub-processor is used, as this will generate a supply chain risk. The safeguards for any onward transfer or use of sub-processor may need to be reviewed, and any US companies engaged in onward transfers will need to conduct a transfer impact assessment as if they were an EU-based data exporter.

In the long term, businesses may consider alternative mechanisms for validating data transfers, such as binding corporate rules, obtaining a certification, or adhering to a code of conduct approved by a supervisory authority (although they all require prior assessment), or considering consent or other derogations in situations where they can be applied.

© 2021 McDermott Will & Emery

National Law Review, Volume XI, Number 140